Microsoft DevOps Solutions: Designing Governance Enforcement Mechanisms

USING AZURE POLICY

John Savill
PRINCIPAL CLOUD SOLUTION ARCHITECT
@NTFAQGuy www.savilltech.com

Learning Objectives

- Implement Azure policies to enforce organizational requirements
- Implement container scanning (e.g., static scanning, malware, crypto mining)
- Design and implement Azure Container Registry Tasks (e.g., Azure Policy)
- Design a break-the-glass strategy for responding to security incidents

Module Overview

Governance requirements

Using Azure Policy

Policy compliance checks

What to do in an emergency!

Every organization has internal and possible regulatory governance requirements.

The usage patterns of the cloud change how governance is enforced and audited which means getting the right solution is critical.

Governance Requirements

Governance requirements are not new to the cloud but the means to enforce likely does require a new approach

Provisioning processes shift to self-service in the cloud in addition to many new types of service and location

Governance needs to be enforced and audited at the cloud API

Azure Policy Overview

Azure Policy provides a means to assess compliance and enforce requirements

Policies are created that consist of a number of rules that are evaluated then an effect used

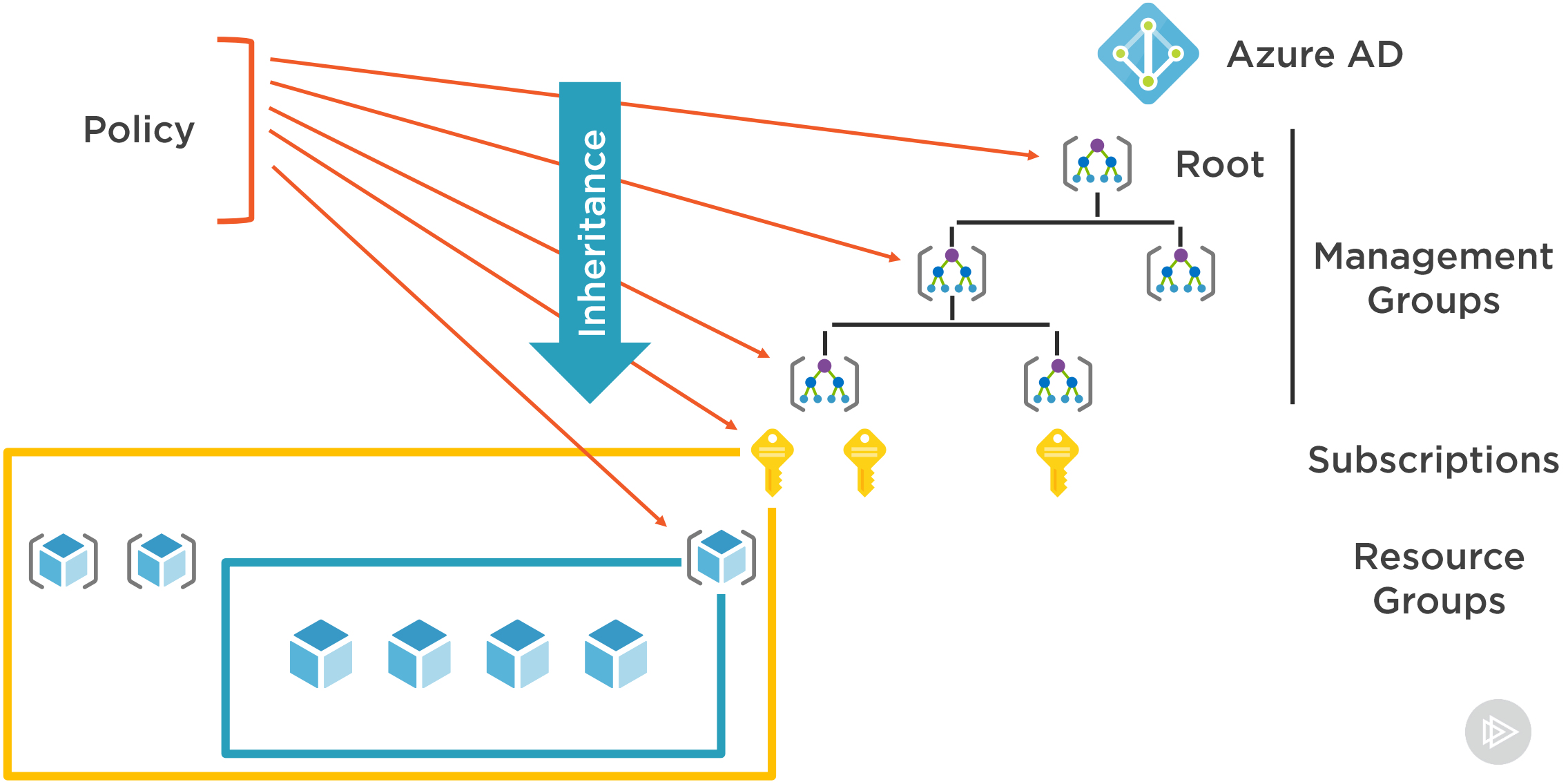
Rules are based on the resource properties exposed as aliases

Effects if the rules match can deny, audit or remediate

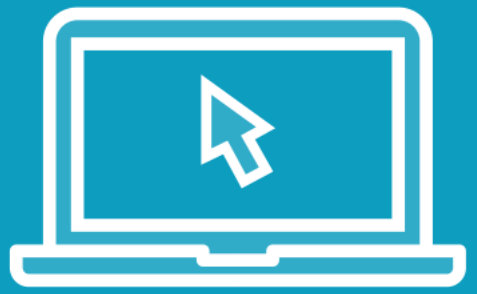
Policies can be grouped into initiatives for easier assignment and compliance status evaluation

This is enforced at fabric level and will apply no matter how resources are provisioned

Policy Assignment



Demo



Azure Policy structure

Assigning Azure Policy

Viewing compliance

Azure Policy for AKS

Azure Security Center integration

Using with Blueprints

Azure Policy Best Practices

Map policies to organizational written policies

Use audit before deny/remediate

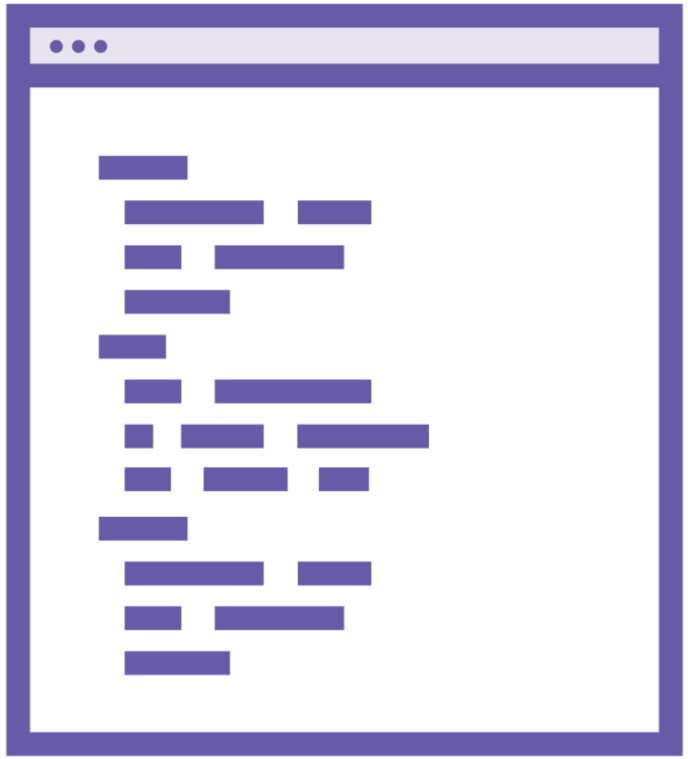
Apply to right level of structure and start small

Broad policies high in structure and tighter as get closer to resource

Have people responsible for tracking compliance

Use good names and descriptions

Azure Policy as Code



Like nearly every Azure resource Azure Policy can be deployed using ARM templates

Separate templates can be used for

- Policy and initiative definition
- Assignment

Azure has a native integration with GitHub to export policy and apply through GitHub Actions workflow

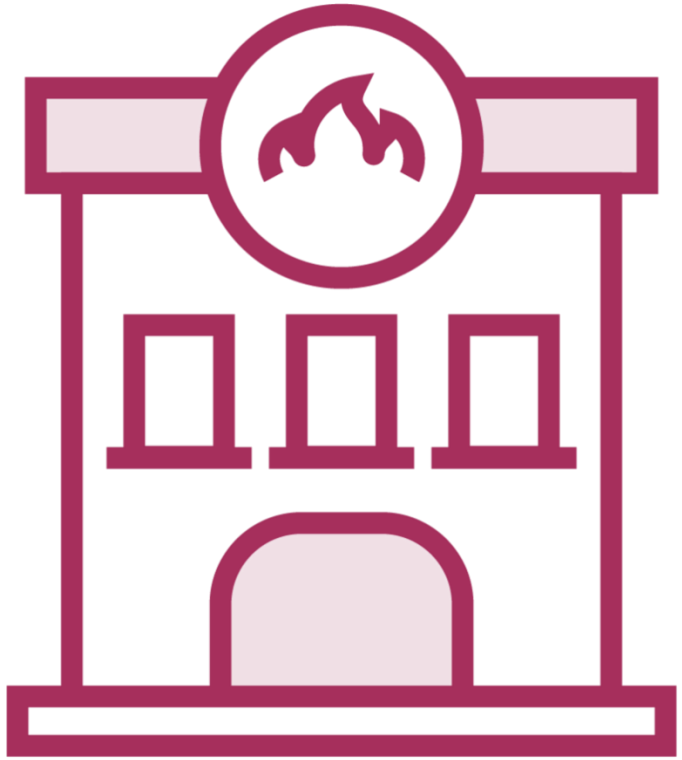
Azure Policy DevOps Integration

GitHub actions has native Azure Policy Action capability

Separate compliance scan action

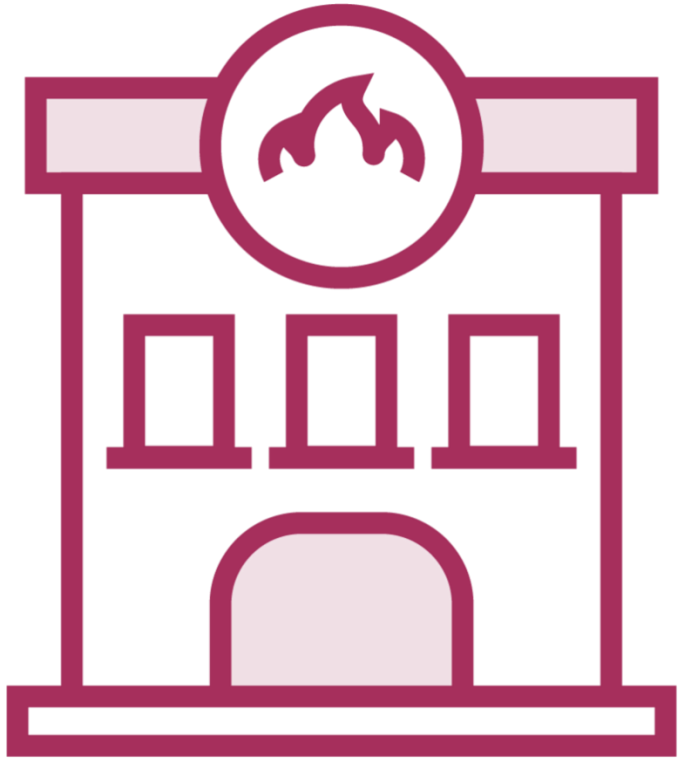
Azure DevOps has native Azure Policy compliance as part of gates for stages

Break Glass Actions for Security Incidents



First do no harm!

Break Glass Actions for Security Incidents



- Security events can be broad in scope
- Have a plan in terms of action and communication
- For an attack on identity or DDoS against identity break glass AAD accounts should exist
- Having password hash sync enables switch to cloud auth if using PTA or federation
- Use solutions that monitor services and apply machine learning to detect threats

Summary

Governance requirements

Using Azure Policy

Policy compliance checks

What to do in an emergency!

Next Up:
Container Governance Tasks